

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the cellular device assigned call
number 614-670-3089, that is stored at premises controlled
by AT&T

Case No.

2:19mj 466

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 229

Prohibitions against chemical weapons

26 U.S.C. § 5861(d)

Possession of explosive device

The application is based on these facts:

See Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: June 13, 2019City and state: Columbus, Ohio

Arnon Beggs
Applicant's signature
Special Agent

Elizabeth Preston Deavers
Printed name and title
Magistrate Judge

Elizabeth Preston Deavers, Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED CALL
NUMBER **614-670-3089**, THAT IS STORED
AT PREMISES CONTROLLED BY AT&T

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Aaron Beggs, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number **614-670-3089**, ("the SUBJECT PHONE"), that is stored at premises controlled by **AT&T**, a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, Florida 33408. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require **AT&T** to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since approximately May 2004. I am currently assigned to the Cincinnati Division, Columbus Resident Agency as a member of the Joint Terrorism Task Force ("JTTF"), where I investigate violations of federal law relating to domestic and international terrorism. Since becoming an FBI agent, I have received specialized training in cyber-crime as

well as on-the-job training investigating criminal activities which include various types of fraud and money laundering. I also have participated in investigations involving violent crime, gangs, kidnappings, fugitives, extortion, crimes against children, and illegal drug trafficking. I am familiar with, and have participated in, all of the normal methods of investigations, including, but not limited to, electronic surveillance, visual surveillance, general questioning of witnesses, use of search and arrest warrants, use of confidential informants, use of pen registers, use of Court Authorized wire and electronic interceptions, use of the Grand Jury process, and use of undercover Agents.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 229 (prohibitions against chemical weapons) and 26 U.S.C. § 5861(d) (possession of explosive device) may have been committed by **JOHN WILLIAM SHADE III** (hereafter referred to as **SHADE**). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

PROBABLE CAUSE

Background of Case

4. This case originated within the FBI after reports of **SHADE** making comments and remarks of a threatening nature on social media via Twitter towards the President of the United States on multiple occasions and one directly towards a local United States Secret Service

(USSS) agent. The tweet involving the local USSS agent came several weeks after the agent attempted a knock and talk at **SHADE**'s residence regarding a recent incident involving **SHADE** at an event involving the Vice President of The United States (VPOTUS). **SHADE** has a history of traveling within and out of state to attend political events as well as protests, and on several occasions, his conduct at these events has resulted in charges related to trespassing, obstructing, invasion of privacy and carrying weapons other than firearms (baton and pepper spray).

5. **SHADE** again came to the attention of the FBI on January 22, 2019 after an arrest and report from Cambridge Police Department. According to the report and witness interviews, **SHADE** threw a baby jar containing an unknown substance smelling of ammonia through the window, injuring at least one person. On **SHADE**'s person at the time of his arrest, among other items, were a flashlight, pepper spray, vehicle keys and cellphone. Officers also collected a Gerber baby food glass jar with an unknown substance inside that was thrown into the residence.

6. On January 23, 2019, Cambridge Police officers executed a search warrant of **SHADE**'s 2011 Black GMC Terrain, which **SHADE** had driven to the scene of the incident, and located, among other items, one box of 9mm ammunition with purchase receipt for Walmart. Cambridge Police obtained Walmart video surveillance footage and after review, officers identified **SHADE** making a cash purchase of the ammunition at the sporting goods counter. Specifically, **SHADE** purchased a Federal 9mm Luger FMJ-RN 100 round box. **SHADE**, however, is a prohibited possessor of firearms or ammunition based on his criminal history.

7. On March 2, 2019, Customs and Border Patrol (CBP) encountered **SHADE** at the U.S. Border/Ambassador Bridge between Detroit, Michigan and Windsor, Canada. During the encounter, and pursuant to CBP's authority, information on his cell phone (614-670-3089) Model LG-H910, serial number 702KPMZ159723, the SUBJECT PHONE, was searched and

seized. FBI/JTTF was later notified of this encounter and the results of the search passed to FBI Cincinnati. On **SHADE's** cellular telephone that was in his possession on March 2, 2019 when stopped by CBP, there was a list titled "Napalm Mollie" and it set forth the following items: glass jar, 50% Styrofoam, 25% fuel, 25% moth balls.

8. On March 22, 2019, law enforcement executed a search warrant at **SHADE's** residence. During the search of the attached garage, law enforcement located an open box on a work bench containing over a dozen glass jars of different sizes with metal lids. Most of the lids had a small hole drilled in the center. The jars contained pink Styrofoam pieces. Additionally, there were gas cans found on the back porch of the residence. Based on my training and experience, the items at **SHADE's** residence are indicative of a Molotov cocktail or napalm bomb, which is an explosive/incendiary device. It appears that the holes were drilled in the lids to allow for a wick to be inserted, which would allow the device to be lit on the outside before placing/throwing the object. Possession of these devices is prohibited under 26 U.S.C. § 5861(d) as explosive, incendiary devices are considered destructive devices and destructive devices are considered within the definition of a firearm, pursuant to 26 U.S.C. § 5845(a) and (f). Additionally, the following evidence was either photographed or collected: a black/green/white fuse cord, 4 Remote Control (RC) Components, Fireworks, Drones, RC Boats, and Fuses.

9. A review of **SHADE's** laptop also seized from **SHADE's** residence revealed a screenshot of what appears to be an electronic communication describing a tentative plan to use chemicals to force an evacuation on a Washington D.C. metro train during the Unite the Right rally in August of 2018. **SHADE** referenced starting at Vienna Station and exiting at the Foggy Bottom station, both stops on the Orange Metro Line in Washington D.C. If chemicals were not used, **SHADE** and several other individuals, not all of whom have been fully identified, planned

to “start dogging Kessler” upon exiting at Foggy Bottom station. Your affiant submits that Kessler was likely a reference to Jason Kessler, the organizer of the Unite the Right rally on August 12, 2018 in Washington D.C.

10. Cell-site information disclosed by AT&T for the time period identified in Attachment B is likely to show evidence of the crimes under investigation because the information can be used to identify whether the SUBJECT PHONE’s user or users were in the Washington D.C. metro area during the Unite the Right rally in August 2018. The information may assist in the identification of co-conspirators and/or victims.

11. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

12. Based on my training and experience, I know that AT&T can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as AT&T typically

collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

13. Based on my training and experience, I know that wireless providers such as AT&T typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as AT&T typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

14. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

15. I further request that the Court direct **AT&T** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on **AT&T**, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Aaron Beggs
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 12, 2019


ELIZABETH PRESTON DEAVERS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **614-670-3089** (“the Account”), that are stored at premises controlled by **AT&T** (“the Provider”), headquartered at 11760 U.S. Highway 1, North Palm Beach, Florida 33408.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider. The Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period August 1, 2018 – August 15, 2018:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. for the time period of August 1, 2018 – August 15, 2018, information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Section 229 (prohibitions against chemical weapons) and 26 U.S.C. § 5861(d) (possession of explosive device) involving **JOHN WILLIAM SHADE III** during the period August 1, 2018 – August 15, 2018.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE
902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by AT&T, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of AT&T. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

b. such records were generated by AT&T's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature